MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DIRECTORS OF DOD FIELD ACTIVITIES
CHIEF INFORMATION OFFICERS OF THE MILITARY DEPARTMENTS
DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS AND COMPUTER SYSTEMS,
JOINT STAFF
CHIEF INFORMATION OFFICERS OF THE DEFENSE AGENCIES
DIRECTOR, INTELLIGENCE COMMUNITY MANAGEMENT STAFF
INTELLIGENCE COMMUNITY CHIEF INFORMATION OFFICER
COMMANDERS OF THE UNIFIED COMBATANT COMMANDS

SUBJECT: DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 7-8170-_____ Information Management

The subject guidance at Attachment 1 is effective immediately. It establishes DoD policies and assigns responsibilities to improve the accessibility, availability, dissemination, and use of information. Attachment 2, “DoD Information Management: Enabling Information Superiority”, is a strategy paper that provides a basis and rationale for much of the policy guidance that appears at Attachment 1. The focus of both documents is on the information itself, and the management activities associated with its creation, dissemination, and use.

My point of contact for this effort is Scarlett Curry who can be reached at 703-604-1574, or by e-mail scarlett.curry@osd.pentagon.mil.

John Hamre
Deputy Secretary of Defense

Attachment 1
Attachment 2

Guidance and Policy for Department of Defense and Intelligence Community on Information Management

References:

(a) DoD Chief Information Officer (CIO) Guidance and Policy Memorandum (G&PM) No. 1-8130-110998, November 9, 1998.

(b) Public Law 105-261, Strom Thurmond National Defense Authorization Act for FY 1999, Sec. 331, “Revision to Title 10 with the added responsibilities of the DoD and Services CIOs”.

(c) DoD Directive Number 8000.1, “Defense Information management (IM) Program”, October 27, 1992.

(d) DoD Chief Information Officer (CIO) publication “Information Management (IM): Information Superiority” (IM Strategic Plan), Version 2.0 (Draft), February 1999.

(e) Joint Vision 2010, “America’s Military: Preparing for Tomorrow.”

(f) Office of Management and Budget Circular A-130, “Management of Federal Information Resources” – Revised (Transmittal Memorandum Number 3), February 8, 1996.

(g) DoD Directive Number 8320.1, September 26, 1991,: “DoD Data Administration”.

(h) DCI Directive 1/1, “The Authorities and Responsibilities of the Director of Central Intelligence as Head of the U.S. Intelligence Community”, 19 November 1998.

(i) DoD Directive 5200.28, “Security Requirements for Automated Information Systems (AISs),” March 21, 1998.

(j) DCI Directive 6/3, “Protecting Sensitive Compartmented Information Within Information Systems,” June 5, 1999.

(k) SM-313-83, “Safeguarding the Single Integrated Operational Plan (U),” May 10, 1983.

(l) DoD Directive O-5205.7 “Special Access Program (SAP) Policy, January 13, 1997.

(m) Secretary of Defense Memorandum U09344/97, 2 June 1997, subject: “Implementation of Subdivision E of the Clinger-Cohen Act of 1996 (Public Law 104-106)”.

(n) DoD Directive 5015.2 “DoD Records Management Program”, 11 April 1997.

1. PURPOSE

This policy guidance establishes Department of Defense (DoD) policy and assigns responsibilities to improve the accessibility, availability, dissemination, use and disposition of information necessary to the execution of the DoD mission.

This issuance:

?? Provides immediate policy guidance under the authority of and in response to direction contained in reference (a.)

?? Responds to Congressional direction relative to the authorities of the DoD and service CIOs established in reference (b.)

?? Interprets, updates, and supplements guidance on management of information as a resource contained in references (c.) and (d.)

?? Assures that Information Management (IM) policies and processes are responsive to the operational priorities presented in reference (e.).

?? Recognizes the unique requirements for Records Management contained in reference (n).

The goal of DoD Information Management is to achieve a seamless secure environment where any authorized user, system, or process has the right information, at the right time, at the right place, from the right source, in a usable format, to make informed decisions and accomplish mission objectives.

2. APPLICABILITY

This guidance and policy applies to the Office of the Secretary of Defense, the Military Departments and their respective services, the Chairman of the Joint Chiefs of Staff and the

Joint Staff, the Unified Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as “the DoD Components”).

3. SCOPE

This policy applies to the management of information that is created or acquired in the course of conducting Department of Defense business or military operations at any time and any place throughout the world.

4. DEFINITIONS

?? **Architecture:** The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time.

?? **Information:** Any communications or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms (reference (f.)).

✍ **Information Management:** The planning, budgeting, manipulating, controlling of information throughout its life cycle (e.g., creation or collection, processing, dissemination, use, storage, and disposition.) (reference (f.)).

✍ **Information Superiority:** The ability to obtain and transmit information unimpeded to any destination as and when needed and to exploit or deny an adversary’s ability to do so. This includes the ability to manage information throughout its life-cycle, i.e., to create, collect, process, disseminate, use, store and dispose of an unimpeded flow of information while exploiting or denying an adversary’s ability to do the same.

?? **Enterprise Solution**: Information Technology (IT) components that are identified and used across the Enterprise to achieve a minimal level of security and interoperability.

?? **Interoperable Mechanisms:** Enterprise solutions employed to process and transport information across the DoD enterprise.

?? **Information Producer:** A person, group, or organization that creates, updates, distributes, and retires information based on their authorized/assigned missions and functions.

?? **Information Consumer:** A person, group or organization, system, or process that accesses and receives information enabling the execution of authorized missions and functions.

?? **Information Profile:** The expression of the requirement for or availability of data, information, or reports enabling the execution of authorized/assigned missions and functions.

?? **Meta-data:** Information describing the characteristics of data; data or information about data; descriptive information about an organization's data, data activities, systems, and holdings (reference (g.)).

?? **Record:** As defined, in part, in Section 3301 of Title 44, United States Code, "Records include all books, papers, maps, photographs, machine-readable materials, and other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them." A record covers information in any medium, and includes operational logistics, support and other materials created or received by the DoD Components in training, contingency, and wartime operations as well as in all routine and peacetime business(reference (n.)).

5. POLICY

It is Department of Defense policy that:

5.1 Information needs shall be identified and documented by information users (hereinafter referred to as information consumers), and understood and acted upon by information creators and compilers (hereinafter referred to as information producers). In this regard:

5.1.1 Information requirements will be described through approved architecture processes and documented in

appropriate operational, strategic, and contingency plans and be reflected as a subset of the DoD IM Strategic Plan and other strategic doctrine such as JV2010.

5.1.1.1 Information requirements will be established through the use of common DoD/IC standard content and format (profiles) mechanisms or common ad hoc requests for information (RFIs) based on validated mission needs.

5.1.2 Information requirements processes will allow distinction to be made between near-term requirements necessary to support day-to-day operations, planning, and decision-making and longer-term information needs against which capital investment decisions are made.

5.2 Consumers are enabled to easily discover, retrieve, and control the flow of appropriate information based upon its characteristics as advertised by producers. This requires that:

5.2.1 Information producers advertise information availability using DoD/IC standard meta-data and producer profiling mechanisms to facilitate consumer research and requests for information.

5.2.2 Information awareness, access and delivery be facilitated through the use of common mechanisms such as producer profiles and source registries. These mechanisms shall include permanently attached attributes, such as authority, classification, and handling restrictions, that enforce effective access and delivery and minimize the risk of improper use of information.

5.2.3 The DoD and IC jointly designate authoritative information repositories and agree upon the distribution (duplication/replication) and disposition (maintenance, retirement, and destruction) of the repositories.

5.2.4 Information producers make information available at the lowest possible security level to ensure the greatest possible use of the information.

5.3 Any component, when acting as an information consumer shall:

5.3.1 Express requirements for information in accordance with the standards and procedures developed under this policy.

5.3.2 Handle information provided under this policy in accordance with attributes assigned by the information producer.

5.4 Any component, when acting as an information producer shall:

5.4.1 Identify information attributes based on standards designated under this policy.

5.4.2 Establish authoritative repositories of information in accordance with mission and function responsibilities.

5.4.3 Advertise information holdings and provide responsive service to validated information requirements.

5.5 Mechanisms for access and delivery shall be implemented that are: interoperable, adhere to accepted standards, provide adequate access control, and ensure that the required information is easily accessed and delivered. In this regard:

5.5.1 Information access and delivery mechanisms and procedures shall follow DoD and IC Information Assurance (IA) regulations. This policy recognizes that special measures and exceptions may be required for protection/handling of foreign intelligence or counterintelligence information, Sensitive Compartmented Information (SCI) (references (h), (i), and (j)), Single Integrated Operational Plan – Extremely Sensitive Information (SIOP-ESI) (reference (k)), Special Access Program (SAP) information (reference (l), or other need-to-know information.

5.5.2 Information requirements shall be satisfied from advertised information over existing or allocated network assets to ensure DoD/IC quality of service and information assurance requirements are met.

5.5.3 Enterprise-wide mechanisms for information access and delivery priorities shall be established.

5.5.4 Access and delivery mechanisms shall meet the rapidly changing operational needs of the Commander. The Commander will have the flexibility to modify subordinate

consumer profiles and access and delivery mechanisms to accommodate his changing environment.

5.5.5 Access and delivery mechanisms shall enable real-time information collaboration between consumers and producers and across functional communities.

5.6 Consistent processes and methods shall be used to facilitate the proper understanding and use of information. This requires that:

5.6.1 Interoperable, standards-based tool sets shall be acquired and maintained to facilitate the discovery, dissemination, and use of information throughout its lifecycle.

5.6.2 The DoD and IC CIOs will monitor and reengineer information management processes as needed to ensure common, effective understanding of delivered information.

5.7 Mission accomplishment shall be basis for assessing the effectiveness of Information Management. To meet this objective, the CIO Executive Board shall:

5.7.1 Establish performance measures, associated metrics, and a reporting process with the participation of the IM stakeholders.

5.7.2 Task appropriate operational entities to measure and evaluate performance against metrics and remedy deficiencies.

5.8 Information meeting the definition of a record, as defined in Title 44, United States Code, is managed in accordance with reference (n.).

5.9 The IC CIO will ensure that the performance assessment effort is applied to the SCI environment.

5.10 Resources shall be planned, programmed, and budgeted to ensure that the provisions of this policy can be achieved.

6. RESPONSIBILITIES

6.1 The Assistant Secretary of Defense (C3I) as DoD CIO shall:

6.1.1 Establish and enforce DoD policy for Information Management in accordance with references (b.) and (m.).

6.1.2 Designate the central governing body for Information Management and assign responsibilities to ensure that the business processes are conducted as prescribed by this policy.

6.1.3 Establish executive agents to oversee specific IM functions, to develop and manage consistent, compatible, and interoperable enterprise solutions, conduct acquisition of standard tools and tool sets, and oversee other acquisition related IM enforcement provisions established by the DoD CIO.

6.1.4 Grant justified waivers from the requirements of this policy.

6.1.5 Establish and enforce data and records management standards and publication, meta-data, and visualization standards that enable Information Management.

6.1.6 Coordinate with the IC CIO to identify and resolve Information Management issues and common requirements, with emphasis on information under the authority of the DCI as specified in references (h) and (j).

6.2 To ensure information is identified, made available, properly delivered, effectively applied, and properly disposed of, the DoD and IC CIOs, acting under the advice of the CIO Executive Board, shall:

6.2.1 Establish common and interoperable mechanisms and standards.

6.2.2 Establish IM priorities based on C/S/A plans and architectures.

6.2.3 Ensure compliance, certification, and audit mechanisms for adherence to IM policies.

6.2.4 Refine the IM business process and establish process improvement methods (e.g., Benchmarking, COTS solutions, Business Case, Unit Costing, and tracking of lessons learned) to evaluate DoD IM.

6.2.5 Provide for the awareness, access, delivery, and understanding of appropriate information across security

boundaries, including the information needs of foreign nationals.

6.2.6 Establish common standards and guidelines for producers regarding information quality, replication, and integrity to support all operational uses and minimize the risk of misuse of the information.

6.2.7 Task, and identify resources for Executive Agents or lead components to define and develop specific standards, procedures, or mechanisms under the oversight of CIO Executive Board.

6.2.8 Establish and coordinate the IM aspects of foreign language information.

6.2.9 Recommend acquisition-related IM requirements.

6.2.10 Recommend awareness, training, education, and career path requirements for IM.

6.3 Chairman of the Joint Chiefs of Staff shall:

6.3.1 In coordination with the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence and the IC CIO, establish joint procedures for the development, coordination, review, and approval of joint information requirements.

6.3.2 Establish joint policies and procedures addressing local commander control of information access and delivery including prioritization, precedence and preemption.

6.3.3 Develop, approve, and issue joint doctrinal concepts and associated operational procedures and guidance, to ensure the satisfaction of mission essential information requirements of U.S. military forces and, as applicable, with coalition and allied forces.

6.4 In addition to responsibilities as a member of the CIO Executive Board, the IC CIO will:

6.4.1 Establish procedures for the development, coordination, review, and approval of information requirements within the IC.

6.4.2 Establish any supporting panels needed to exercise unique responsibilities of the DCI for the management of SCI information.

6.4.3 Oversee enforcement of common IM processes, standards, and procedures within the IC in support of the DoD mission requirements and enable DoD intelligence agencies to meet requirements of this policy.

6.4.4 Represent IC interests and coordinate IC positions relative to the collaboration with foreign nationals in DoD information management processes.

6.4.5 Provide expertise on the foreign language aspects of IM.

6.5 The OSD Principal Staff Assistants (PSAs) shall:

6.5.1 Establish procedures for the development, coordination, review, and approval of information requirements in their functional areas.

6.5.2 Ensure that these policies are implemented in their areas of functional responsibility.

6.6 Commanders in Chief (CINCs) of the Unified Commands shall:

6.6.1 Implement IM policies and procedures within their areas of responsibility (AOR) consistent with this policy.

6.6.2 Through their participation in the CIO Executive Board, identify, prioritize and document information and IM process requirements (right information, place, time).

6.6.3 Provide performance assessment on the satisfaction of their warfighting information requirements.

6.7 Designated Enterprise Executive Agents shall:

6.7.1 Provide the staff and other resources needed to execute their IM responsibilities as tasked by the CIO Executive Board.

6.7.2 Provide status reports and receive guidance and support from the CIO Executive Board in meeting those responsibilities.

6.8 The Heads of the DoD Components shall:

6.8.1 Ensure compliance with this policy.

6.8.2 Establish procedures for the development, coordination, review, and approval of information requirements in their mission areas.

6.8.3 Establish and enforce an Information Management policy for their component consistent with this policy.

6.8.4 Revise component IM policy in accordance with guidance established by the CIO Executive Board.

6.8.5 Accept IM executive agency responsibilities.

6.8.6 Plan, budget, and execute adequate resources in support of IM.

6.8.7 Specify Information Management requirements and standards in the design, acquisition, installation, and operation of information systems and infrastructure.

6.8.8 Ensure that awareness, training, education, and career paths support IM.

6.8.9 Ensure that information requirements are documented and validated in accordance with DoD policy, including approved architecture processes and frameworks.

DOD INFORMATION MANAGEMENT: ENABLING INFORMATION SUPERIORITY

A STRATEGY PAPER
OF THE
GNIE IM PANEL

Version 4.0
13 September 1999

TABLE OF CONTENTS

LIST OF FIGURES

Purpose

This paper defines a strategy for managing, within the context of a Global Information Grid (GIG), all information generated, acquired, and used by the Department of Defense (DOD) and by DOD Components in support of decision-making and mission accomplishment for the purpose of establishing Information Superiority. It defines a process called Information Management (IM) – one of several processes so named -- that deals specifically with that information, independent of its form and of the media by which it is conveyed. It positions IM within an overall Information Technology/Information Resources Management framework and differentiates the GIG IM process from all others. It establishes a vision for the desired end-state. The IM strategy proposed herein addresses a business model with five business process areas. Within each IM business process the current environment is described, followed by a list of recommended actions that will enable the DOD to realize the proposed GIG IM vision.

Background

In recent testimony before the House Armed Services Committee, several DOD senior leaders articulated the importance of information superiority to our national defense; discussed the contribution of information infrastructure in achieving information superiority; and, provided their joint or Service perspective of what should and is being done to further this goal.

According the Deputy Secretary of Defense, “Information superiority is essential to our capability to meet the challenges of the 21st Century. It is a key enabler of Joint Vision 2010 and its four fundamental operational concepts of dominant maneuver, precision engagement, full dimensional protection, and focused logistics. Each of these concepts demands the capability to collect, process, disseminate, maintain and protect an uninterrupted flow of information.”

This strategy addresses the collection, processing, dissemination, maintenance, protection, and use and disposition of information, not the infrastructure that supports it. It focuses on the components of a business model for effective management of information. Major efforts are underway within the Department to develop policy and guidance on specific aspects of Information Management (for example, Information Dissemination Management (IDM) and Records Management (RM)). These efforts are cited in this strategy and the guidance and policy derived from it, but are not repeated to avoid duplication.

Much attention, in the Global Information Grid (GIG) efforts, has been given to the infrastructure that processes and moves information around. Is there enough bandwidth at the right

places? Are the applications efficient and effective? Is there enough processing power at the right place? Much less attention has been given to information as an asset. What information is needed? Where is it located? What must be done with it before it is useful? Is it the right information? The strategy outlined in this Paper provides a means of answering these questions through the establishment of five IM business process areas that will be outlined in Section 7.0.

To achieve information superiority, information must be managed so as to drive and justify the building and maintenance of an infrastructure to handle it. This strategy deals with content -- the information asset -- and the Enterprise-wide guidance necessary to assure that the right information can be identified, located, and brought to bear on the decision/mission at hand.

Strategic Planning Approach

Improvements in information management require an overarching view of the current IM process, a vision of the desired end-state, and a set of clearly defined goals that must be achieved to reach it. The means of achieving the goals, in the form of specific actions that must be taken across the DOD, will be identified. The result is the articulation of a business model for information management. The model addresses the definition of requirements, means of advertising and labeling information, mechanisms to support information access and delivery, processes that support the proper use of information, and the overall management and governance required.

Information Management Environment

The DOD information management environment is complex and confusing. Different concepts and entities are referred to by the same or similar names. For instance, information, as referred to in this strategy, can be synonymous with data, information, or knowledge. These are the entities of the environment that must be managed in order to support effective decision-making and mission accomplishment and provide the opportunity for information superiority. These are the entities that are operated on by various users, systems, and/or processes in order to make those necessary decisions and accomplish assigned missions.

Information

The simplest of the entities is data. Data are symbols that express statements about the world (e.g., words, numbers, pictures, etc.). When organized, or retrieved, by some user, system, and/or process, within some context (e.g., order, grouping, some specified relationship, some specific purpose), data becomes information. Information is data elevated by context. When information is organized and abstracted to have

useful, predictive, and explanatory power for the user, system, and/or process, that information becomes knowledge (e.g., experience, values, expert insight, etc.). Knowledge is information known and understood to apply to a certain decision, or mission area. Knowledge is information elevated by cognition. Decision Support, on the other hand, is information applied to specific decision tasks or mission areas and/or associated actions. Decision support is applying the right knowledge for the decision task or mission area, at hand. In essence: information is purposefully constructed from data; knowledge is discovered with the understanding of information; and, decision support is the appropriate application of data, information, or knowledge to meet mission or policy objectives. There are no hard lines between any of these classifications. Actually, they are merely higher levels of abstraction from the initial raw data and decisions are made based on any one of them based on the situational need. Figure 1 illustrates this hierarchy of entities from data to knowledge and their relationship to decision support. In this strategy, these entities are collectively referred to as information.

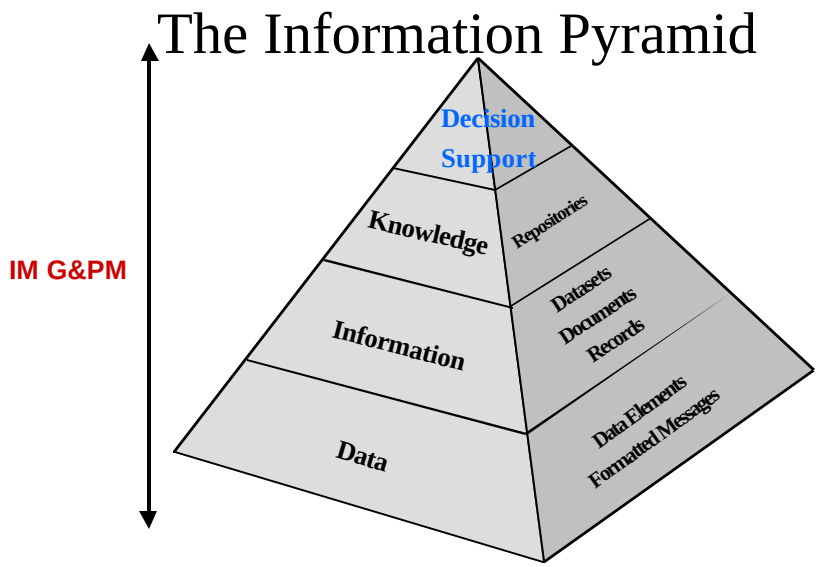

Figure 1. Hierarchy of Information Entities

Information Management

There are different activities associated with the management and use of each entity. These activities are generally categorized as data management, information management, knowledge management, and decision support. Figure 2 lists some

of these activities and illustrates their relationships, again noting the increasing level of abstraction associated with progression from data.

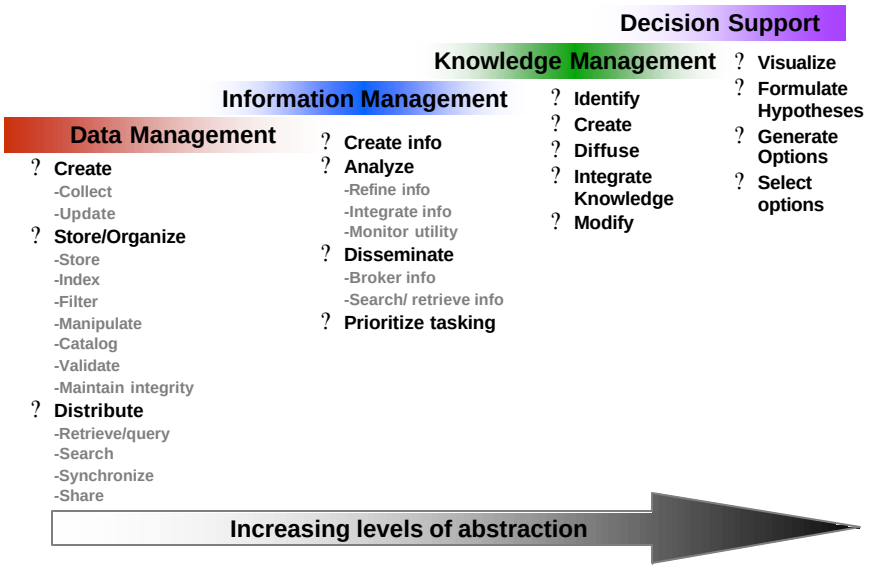

Figure 2. Activities Associated with Management and Use of Information Entities

These activities relate to the life and use of information as illustrated by the life cycle diagram at Figure 3. Information, in whatever form, is created or retrieved on the basis of an identified need. That information is then disseminated to the requiring user, system, or process and used in support of the planned decision or mission. Based on the success or failure of that use, and the nature of the information, it is either updated or not and either stored for future use or destroyed.

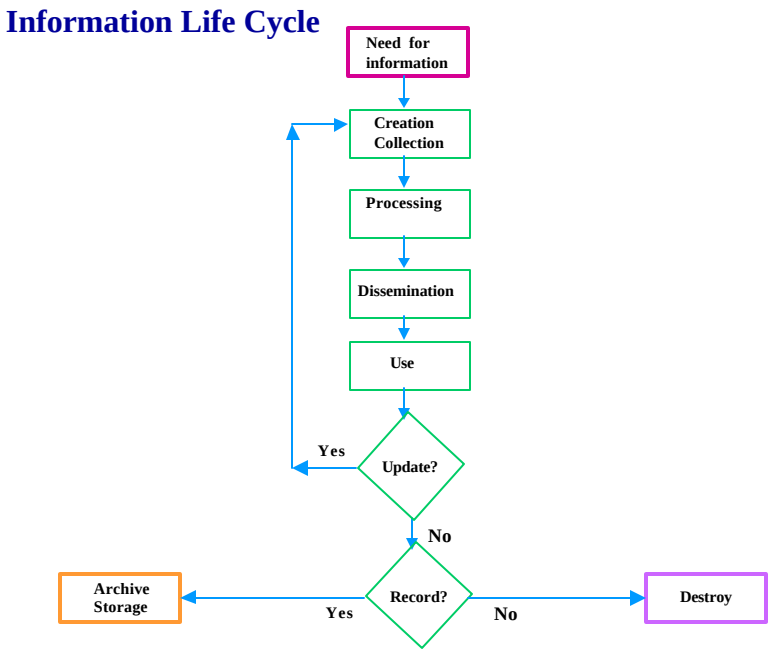

Figure 3. Information Life Cycle

This set of activities, illustrated, in part, in Figures 2 and 3, constitute the process referred to herein as Information Management (IM). These are all general activities operating on and manipulating information, independent of the tools, systems, and technologies that actually perform any given operation for a specific decision task or mission area. These latter are generally referred to as Information Technology (IT) and are considered to be, along with the information, part of the total information resources of DOD.

Positioning IM in the Context of GIG

The diagram shown in Figure 4 is a general model showing the components of GIG, as defined in the Enterprise Architecture Framework (EAF) that was developed by the GIG Enterprise Computing Panel. The Enterprise Operations (EO) Thrust Area Leaders have designated the EAF, an extension of the C4ISR Architecture Framework v2.0, as the common framework for all EO Panels. The EAF focuses on a Computing and Network Architecture Framework (CNAF). As this diagram illustrates, Information and its Associated Applications utilize the CNAF components to meet the information transfer needs of the Functional Communities of Interest (FCOI). The access and delivery of information is facilitated by Enterprise Solutions that are common to all FCOIs. Essential for interoperability are Information Technology Standards, which are positioned as the foundation of the diagram. As will be discussed in Section 7.0, the adoption and enforcement of appropriate standards is a fundamental principle of this IM strategy.

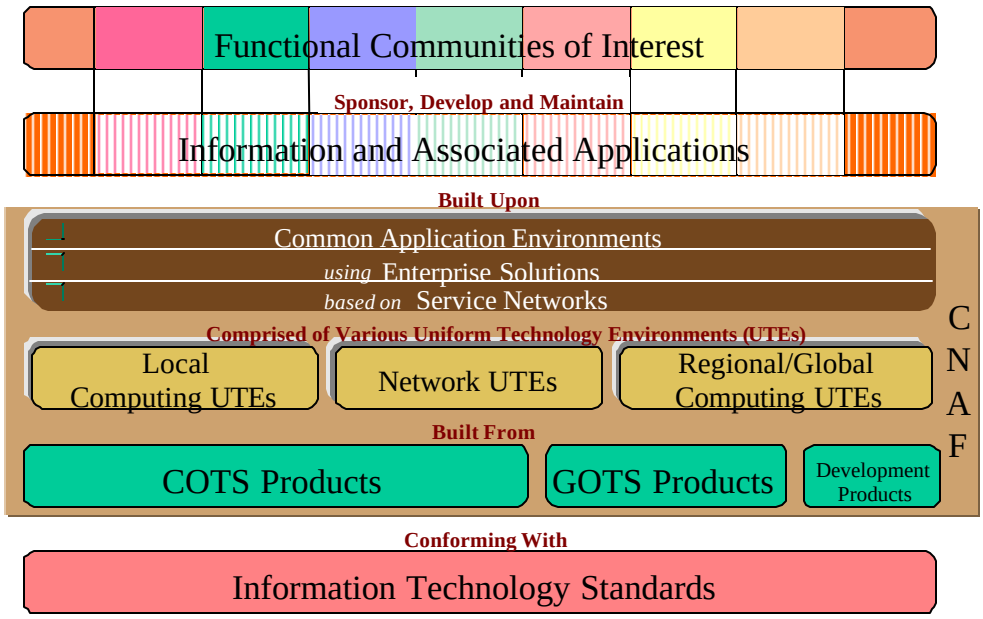

Figure 4. Information Management Positioned Within the GIG

Relationship to DOD IT Strategic Plan

The Clinger-Cohen Act of 1996 (formerly the Information Technology Management Reform Act of 1996) mandates that DOD improve its day-to-day mission processes and properly use IT to support these improvements. The DOD has published a Strategic Plan to address these improvements. The initial IT Management Strategic Plan was published in March 1997. The second version is currently in draft form. It has been renamed Information Management (IM): Information Superiority – IM Strategic Plan, for short.

Four (4) goals are established in the DOD IM Strategic Plan:

1. Become a mission partner;
2. Provide services that satisfy customer information needs;
3. Reform IT management processes to increase efficiency and mission contribution;
4. Ensure DOD's vital information resources are secure and protected.

The IM strategy that is presented within this paper supports these goals. For example:

?? DOD IM Strategic Plan Objective 1.3, *"Move Towards An Information Marketplace"*, lists strategies on focused information, developing and applying methods and tools for helping a customer determine the value of information to their missions and tasks, and reducing the "glut" of

information. This objective is supported in Sections 7.3 of this Strategy Paper.

- Objective 2.4, *"Introduce New Paradigms"*, lists strategies on a collaborative environment to help a user find information from a variety of sources known to the infrastructure but not to the user and simplifying requirements detail and reducing lead times for new information requests. This objective is supported in Sections 7.2 and 7.1.
- Objective 3.1, *"Institutionalize Clinger-Cohen Act Provisions"*, includes a strategy aimed at maintaining a customer/user focus. This objective is supported in Section 7.1, which emphasizes the importance of the customer's role in the information requirements process.
- Objective 4.3, *"Enhance DoD Information Assurance Operational Capabilities",* lists strategies for establishing information protection processes and standards for the Enterprise. This objective is supported in Sections 7.2 and 7.3.

These examples are not exhaustive; they are included here to illustrate the harmony between the DOD and GIG documents relative to IM. The key difference is the level of detail; the GIG plan outlines specific actions required for effective IM. Since the DOD plan encompasses more that just IM as defined in this Paper, it is at a higher level of detail. Many of the strategies in this Paper will directly support the objectives of the DOD Plan.

Vision

A vision for IM is required to properly scope a success oriented IM strategy. The IM vision is:

> Any authorized user, system, or process has the right information, at the right time, at the right place, from the right source, in the right format, to make informed decisions and accomplish mission objectives.

This vision is aligned with the DOD IT community mission from the IM Strategic Plan and supports the Information Superiority objective of JV2010.

IM Business Model

The actual business of managing information is one involving information, information producers and consumers, and a variety of enabling mechanisms. This is depicted in the diagram in Error! Reference source not found.. Information producers/providers and information consumers operate on information to make decisions and accomplish mission assignments. There are, in fact, five business processes at work here:

- Identify information requirements
- Identify information availability

?? Implement mechanisms to access and deliver information
?? Facilitate information use
?? Provide overall process management

These IM business processes, taken together, constitute an IM Business Model. These business processes are the thrust areas for the IM Strategy proposed in Section 7.0. In relation to Figure 4, these processes support the Functional Communities of Interest by providing the essential elements required to sponsor, develop, and maintain information and its associated applications.

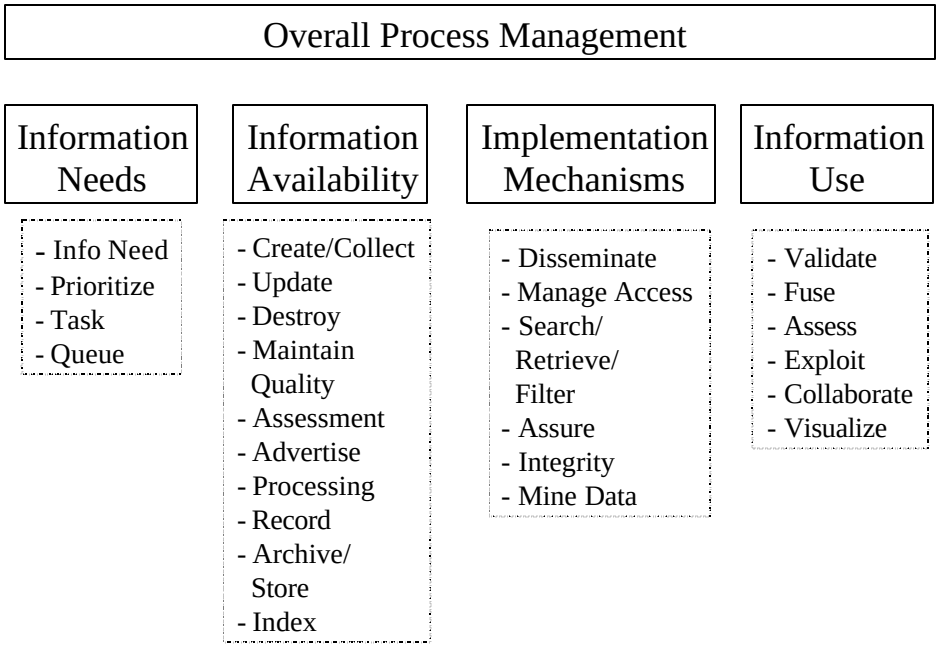

Figure 5. IM Business Processes

The IM business processes should be managed through a collaborative governance process that includes the information providers, consumers, protectors, and information technology support. Lastly, they need to support a wide range of operational, policy, and business needs including: command and control, the demanding sensor-to-shooter concept, battlefield situation awareness, intelligence, personnel, finance, logistics support, records management and electronic commerce.

IM Strategy

To successfully manage information as a resource within the DOD, a set of goals and strategies that address all of the required functions and processes within the IM business model and allow participation by all of the information stakeholders are identified below. The goals are comprehensive, providing end-to-end support for the gathering, provision, use, and eventual disposition of information. An essential element in the achievement of these goals is the adherence to DOD policy,

procedures, and guidance with regard to information technology architectures and standards. This will be discussed in greater detail, but is a fundamental principle that must be understood. DOD leadership must be committed to the implementation and enforcement of architectures and standards for successful IM and the achievement of Revolution in Business Affairs/Revolution in Military Affairs (RBA/RMA). The goals map directly to the IM Business Model (Figure 5) and the model's associated business processes; the thrust areas in which the goals are developed are, in fact, those same business processes:

- ?? Identify Information Requirements – assures that information requirements from all consumers are known to the information providers based on mission needs
- ?? Identify Information Availability – provides the means to identify what is available and its qualities relative to needs.
- ?? Implement Mechanisms to Access and Deliver Information – provides the means to gain access and assure delivery of information to the appropriate information user.
- ?? Facilitate Information Use – provides enterprise-wide, interoperable standardized processes and methods that facilitate the end use of the information.
- ?? Provide Overall Process Management – the collective management of the information management business process in accordance with policy and strategic direction.

Each of these five thrust areas is described in greater detail below. A brief description is provided, followed by a goal statement. This is followed by an assessment of the current situation and a set of implementation strategies that will help achieve the goal.

Identify Information Requirements

The expression of information requirements in terms that are understood by both information consumers and producers is essential. The articulation of requirements needs to be coordinated within a common framework that minimizes opportunities for misinterpretation.

Goal Statement

Information needs are identified and documented by consumers, and understood and acted upon by information providers.

Current Environment

There are many issues related to the identification and understanding of information needs. From an operational perspective, Commanders, decision-makers, functional managers, and other information consumers may not be able to adequately define the requirements necessary to perform their assigned

tasks and missions. They have only limited means to share needs and collaborate with each other and information providers, thus resulting in duplication of information requirements and, in turn, duplicative information systems and technologies. Because requirements-definition is carried out in a stovepipe manner, information needs cannot be prioritized across the enterprise. Lack of a common environment, does not allow information providers to provide a means for information consumers to obtain required information to perform their mission.
From a more strategic perspective, information requirements are not developed in consonance with Enterprise-wide and DOD level strategic plans and there is no enterprise-wide architecture within which to frame these requirements. Additionally, there is no uniformly accepted approach to document information needs. This encourages the development of information systems and technologies that do not meet common standards, do not share common data definitions, support a single function, and are not interoperable. Multilingual requirements are frequently ignored or forgotten.

Recommended Strategies

Develop and manage information requirements through architecture-driven approach.

Architectures provide the primary, long term denotation of the mission and related IT support. Improvements in the execution of military tasks require advanced technology and robust new applications. This requires:

?? Adoption of an integrated architectural framework, in accordance with the C4ISR Architecture Framework v2.0, for operational, systems, and technical architectures that ensures interoperability and uniformity and strengthens the linkage between weapons, information systems, and mission capabilities.

?? Endorsement of a disciplined environment whereby the roles and responsibilities of generating, integrating, and migrating to such architectures are institutionalized and rigorously enforced.

Develop enterprise-wide standard sets of information requirements for establishing tasks and functions.

Today’s systems are too narrowly focused and stove-piped. Management of the end-to-end infrastructure must support the goal of seamless integration and modernization. This requires:

?? Establishing standard sets of information that build upon identified information requirements to suit specific needs.

?? Developing a standard integrated framework mission needs validation process
?? Developing operational, strategic, and contingency plans that are shared across the enterprise and emphasize the characteristics of required and common information.
?? Establishing standards that equate to mission achievement and permit measurement of performance.

Develop and adopt enterprise-wide standard user profiles and priority schema.

The current infrastructure needs to fully utilize existing assets. Therefore, increased efforts should be made by producer and providers to identify and diminish duplication while promoting opportunities for the use of joint assets. This requires:

?? Establishing profiling standards.
?? Producing, storing, and readying information for access according to user profiles.
?? Developing tables that identify existing and potential consumers and producers of the same information.
?? Establishing standard information requirements based upon situational considerations or the operational environment.
?? Matching prioritization schemes to fit operational needs.

Create common conceptual data models.

Sharing data across the enterprise is crucial to interoperability and quality data. This requires:

?? Synthesizing, organizing, and sharing requirements for secure, joint information repositories under the purview of centrally controlled data administrators.
?? Creating common, robust sets of core data items/models.
?? Creating metadata models that supply the critical information pieces that are representative of the data resident in databases, data warehouses, or other repositories.

Identify Information Availability

A major objective of the information management business process is to ensure the end user has the means to identify what is available and can compare its qualities in terms of satisfying mission needs.

Goal Statement

Consumers are able to easily discover, retrieve, and control the flow of appropriate information and its characteristics as advertised by producers.

Current Environment

Currently, information is not readily available across organizational boundaries without the creation of additional manual processes or automated mechanisms. The result is that information exists but is not readily accessible to consumers in other organizations. There are several causes:

- *Limited accessibility*. The process for network connection has proceeded slowly, thus limiting the consumer's ability to reach across networks to access information. Further, not all databases are distributed on a network.
- *Security boundaries*. The information might be classified and not made available to users who have a legitimate need to know.
- *Lack of awareness*. There are no commonly accepted means for advertising to keep information users informed of the existence of information and how to access it.
- *Inadequate Interoperability*. Current systems do not interoperate well and data are generally not sharable among Communities of Interest. Contributing factors are:
  - The need for format conversion utilities.
  - Incomplete data element standardization. There still are many domains (subject areas) where data elements have not been thoroughly modeled, normalized and standardized.
  - Sub-optimal implementation of standard data elements. Although very successful in populating the Defense Data Dictionary System (DDDS) with data elements for many domains, DOD organizations have been slow to convert shared data stores to standard formats.
  - Lack of coordinated architectures. Without coordinated architectures, it is very difficult to understand business rules, relationships between applications/systems, between data elements, and information exchange requirements.
  - Overprotection. In many cases, the information cannot be easily accessed due to excessive access control constraints.
  - Lack of multilingual fonts, interoperable foreign language software, and language-related metadata
- *Copyright and the cost of information.*

Recommended Strategies

Implement a standards-based metadata approach to assist in the discovery, retrieval and control of appropriate information

- Adopt standard markings for information content, security classification, and releaseability.

?? Establish "libraries" where metadata and data models can be stored.
?? Develop automated data profiling algorithms to optimize and ensure high priority information requests are filled.
?? Develop consistent and meaningful schema to relate relevancy of search results
?? Emphasize characterization of information products by their producers
?? Identify standard metadata requirements for information.
?? Align and synchronize with DDDS.

Provide the commander or manager the flexibility to select the information he needs when he needs it

?? Develop flexible communications systems/networks that permit prioritization of information flow
?? Develop means for information/data to be prioritized, such as messages today, to ensure high priority data requests are filled first.
?? Develop means whereby a qualified user can discover and access information without prior knowledge of its existence, location, or classification (e.g., random word search)..

Establish registry of authoritative sources of information.

?? Develop a system that will index and organize advertised information.
?? Encourage, and provide incentives for, collaborative development of data repositories and data storage.
?? Create catalogs of information stored.
?? Develop standard of advertising information.
?? Provide for collateral advertising of special access information wherever feasible.
?? Develop new and/or select standard commercial search engines.
?? Implement an effective records management program.
?? Publish to the enterprise and beyond (as required) those libraries, warehouses, repositories, etc. that hold the information.

Adopt a standard access authorization model utilizing enterprise-wide user profiles.

?? Develop means to centrally validate users' requirements, access levels, delivery priority
?? Adhere to accepted standard access authorization processes
?? Implement enterprise-wide standard user profiles

- Produce, store, and make ready information for access according to user profiles
- Build and disseminate databases of user profiles
- Establish profiling standards
- Develop tables that identify existing and potential consumers and producers of the same information

Implement Mechanisms to Access & Deliver Information

Implementation mechanisms are hardware, software, IT standards, and processes that enable information to be readily located, accessed, and delivered in a secure manner, in the right format, when and where needed. They provide for the processing of information in common ways to meet common uses; for the search, retrieval, filtering, summarization, and mining of information from existing holdings; for the dissemination of information as it is created; and, for the delivery and integrity of the information. These mechanisms help to manage "information overload".

Goal Statement

Consistent and interoperable mechanisms that adhere to accepted standards are in place to ensure required information is easily accessed and delivered.

Current Environment

Implementation mechanisms necessary to insure the accurate, timely, and secure flow of information are not fully in place. Information is isolated by organizational boundaries, as well as by sensitivity and classification levels, thus inhibiting attempts to discover and access information relevant to a particular need. There are no common processes for managing access to information nor is there a comprehensive access management method.

Information providers and information consumers have not agreed upon nor implemented common technology and or data (metadata) standards. There is a lack of agreement between information providers and consumers on the mechanisms (e.g., profiles) to guide information access and delivery. There is little agreement on the amount, types, and operational use of information filters to support various operational concepts and policies for information delivery (push, pull, etc.).

The means to gain awareness of appropriate information and deliver it to authorized users across security boundaries are slow to emerge and costly to implement. Lastly, there is an overwhelming reliance on technology to solve what otherwise are cultural and policy issues. Some of this reliance on technology can be assuaged through more effective governance of the means to access and deliver information.

Recommended Strategies

To address the implementation mechanism shortfalls, the following major actions are needed.

Define requirements for successful system and network operations that enable the secure and reliable delivery of required information.

?? Establish Network Operations Centers that support both the use of intelligent push and the demand pull of information.
?? Develop mechanisms to dynamically allocate network (infrastructure) services to satisfy information needs.

Provide tools and techniques that facilitate the compilation, filtering, correlating, cataloging, caching, distribution, and retrieval of information needed to accomplish a mission.

?? Establish common producer/consumer procedures for developing information access and delivery profiles
?? Adopt uniform policies and standards to process, record, disseminate, store, archive, and retire/destroy information
?? Provide a means to share information on successful information access strategies and tools.
?? Exercise the use of experimentation to achieve small-scale mission-specific cases and adapt large-scale procedures to those needs.

Provide the secure means to access and deliver all types of required information. Activities necessary to accomplish this objective include:

?? Develop security procedures that encompass the total information requirement from cyberspace to voice to other networks to standalone processors
?? Establish mechanisms to optimize the use of information resources consistent with the Commanders policy
?? Develop mechanisms for information access and delivery that support component operational and system architectures developed in accordance with the C4ISR Architecture Framework v2.0
?? Ensure appropriate information security classification
?? Provide information access and delivery mechanisms across security boundaries.

Facilitate Information Use

The end objective of the information management business process is to ensure that the information is understood and can

be effectively employed to perform mission tasks. These tasks range in level of difficulty and complexity including:

?? The direct delivery of specific pieces of data in prescribed formats to specific systems and applications;

?? Facilitating rapid, complete and common understanding of information using methods such as visual display for situation awareness; and,

?? Supporting the aggregation and synthesis of information into knowledge that can be used to develop strategy and policy.

Functions that support information use include validation, fusion, correlation, assessment, visualization, and collaboration. These functions support both the immediate use of information for decision-making and a wide range of knowledge management and decision support capabilities.

Goal Statement

Consistent processes, tasks, and methods that facilitate rapid, complete, and common understanding and proper use of the information.

Current Environment

There is a wide diversity of means to interpret, assess, manipulate, and display information across functional disciplines, often leading to uncertain or conflicting conclusions from commonly available information.

Consumers often lack or have inconsistent means to validate information. There are no generally accepted indicators of information reliability/quality (timeliness, authority, currency, and credibility of source, traceability). Consequently, there is an uncontrolled duplication of information and widespread delivery of unneeded information (overload). There is a lack of common situationally appropriate visualization tools, often leading to an inability to integrate information of various types from various sources in a common display. Furthermore, there is a lack of appropriate data correlators to reduce redundancy of information provided.

The application of automated inference engines and limited fusion capabilities are inconsistent since each functional area tends to solve the same need in different ways. This situation is compounded by the limited means to collaborate among information providers and consumers. Consequently, the opportunity to resolve conflicting information or ambiguous results, to prevent the misuse of information, and to provide immediate feedback to producers is very limited.

The end result is an information environment that requires extensive workarounds, conversion processes, and patchwork solutions to apply information. This, in turn, significantly increases the risk of error in integrating information and the

complexity and number of skill levels required and, hence, the costs of training. The rapid, complete and common understanding of the required information must be facilitated in order for Information Superiority to be achieved.

Recommended Strategies

Adopt a uniform set of rules for information quality and evaluation.

This is a key element of an integrated strategy for using information. It would allow both information producers and consumers a common way of expressing and evaluating uncertainty and assessing the proper use of information.

Improve collaboration processes among users as well as between users and producers.

Secure, effective means to collaborate will provide the opportunity to ensure that information is complete and accurate and will help avoid or minimize misuse or misinterpretation in critical decision-making situations. It is important to recognize and adjust for the difference in semantic context of the consumers and producers.

Develop standard guidelines and measures of effectiveness for the implementation of new and emerging technologies.

A means to ensure that emerging technologies are adopted and applied in standard ways to common information problems is needed. Technologies must be sought that improve the communication of knowledge from the producer to the consumer.

Establish guidelines on information duplication/replication.

Poorly controlled proliferation of information can result in significant errors in applying the information since the opportunity to use information that has been modified or is unsynchronized with the source is very high. Agreement is needed on which information should be replicated (for example, across security boundaries) and how it is to be synchronized.

Develop means of detecting misuses of information and establish policy for noncompliance.

Wrong, improperly understood or misapplied information can be worse than the absence of information. Mechanisms must be developed that find and correct errors in fact, understanding, or application of information. Information must not only be accurate but it must also be provided with sufficient context that it is rapidly and clearly understood. Furthermore, the

consumers must have sufficient background and training to avoid misapplication of the information.

Management Processes

Management processes are those activities that enable the successful implementation, operation, and control of an information management program. These activities include strategic planning, policy promulgation, resource identification and allocation, and governance.

Goal Statement

Effective governance and sufficient resources are in place to ensure information is identified, made available, properly delivered, and effectively applied.

Current Environment

Information is central to the way we fight, and is absolutely critical to the support of our warfighters and policy makers. Clearly, the success of our warfighters and those who support them depends on an effective Information Management program. We must ensure that we have effective governance and sufficient resources in place that provide for information being identified, made available, and properly delivered in a cost-effective and affordable manner.

It is not clear that the current environment provides such assurance. For example, while we have plans, policies, management structures, and control processes in place, the effectiveness of these are constantly being questioned – internally and externally.

In order to improve our current situation, we need to ensure that:

?? Information management planning reflects a strong linkage to overarching DOD plans as well as plans for the Warfighter and those who support them.

?? Policies and procedures are up-to-date and keep pace with modern practices and technology.

?? Management structures, at all levels, promote a collaborative approach to the coherent management of information and the technology that supports it.

?? Roles, responsibilities, and accountability are clear, and not elusive.

?? Management and oversight control processes are effective for assessing the costs and risks of proposed IM/IT initiatives.

?? Projects are consistent with coordinated and approved architectures and standards.

?? Measures of performance are institutionalized.

?? Strong enforcement mechanisms are in place, and there is unwavering commitment to using them.

?? The information and associated technology that we have are visible throughout the enterprise.
?? There is a concerted enterprise effort to utilize successful industry practices and to benchmark our processes against industry.

Recommended Strategies

Institutionalize an IM strategic planning process that reflects a strong linkage to the DOD strategic plan, joint warfighter plans, and business/functional area plans.

The IM strategic planning process and associated Plan should horizontally and vertically integrate DOD information management activities, provide the foundation to align expenditures to mission-and functional-related outcomes, and reflect enterprise-wide acceptance and commitment to its execution.

Establish policies, assign responsibilities, and delegate authorities that provide for effective information management.

Such polices should provide a realistic and sound foundation for the Department attaining and maintaining information superiority (e.g., create, collect, process, disseminate, use, store, and dispose of an unimpeded flow of information while exploiting or denying an adversary's ability to do the same) at an affordable cost. Inherent in these polices must be established roles and responsibilities, enforcement mechanisms, and responsibilities and accountability for enforcing them.

Establish governance processes and management structures at all levels that reflect a team-oriented, collaborative, and enterprise-wide approach to information management.

The following key constructs are essential: effective managerial leadership; efficient management and organizational structures; personnel competence; delegation of authority and responsibilities at the lowest possible levels to the maximum extent practicable; as well as sound doctrine, policies, procedures, budget, reporting practices, and oversight.

Establish and maintain inventories/repositories of information and associated information technology assets.

Such inventories provide the means to: establish accurate baselines for assets; perform assessments of existing capabilities to support mission and functional objectives in a cost-effective and efficient manner; design/improve the

information infrastructure and architectures; and support decisions regarding whether to undertake new investments.

Include IM requirements in capital planning and investment control process.

This process must: establish a budgetary means (e.g. Information Management Program Element) to support IM planning, programming, and operations; centralize funding for requirements that are common across the enterprise; establish a means for examining and making trade-offs among competing proposals; and maximize leverage on investment.

Design programs aimed at acquiring, developing, and retaining a well-trained workforce that is knowledgeable about information management principles, practices, and procedures.

Establish an information management career (sub) specialty and supporting training program similar to the Defense Acquisition Education, Training, And Career Development Program (DODD 5000.52) to ensure IM workforce competency.

Summary and Next Steps

The next major challenge for IM is the successful implementation of the strategies of this Paper and those of the DOD IM Strategic Plan. The goals used as the foundation for this Paper were developed through collaboration and consensus of IM representatives from across the DOD and IC. Although consensus was reached with regard to the essential processes required for successful IM, there is agreement that several areas need further refinement to round out the plan:

- Meaningful Metrics: High level indicators of success were proposed, but detailed measures of DOD’s steps toward improvement are required.
- Leadership: The overall governance of the GIG is currently being defined. The CIO Executive Board referenced in the IM G&PM will be a key component in the successful reengineering of IM practices. Regardless of the overall governance structure and processes established, the IM Panel unanimously agrees that IM needs strong leadership from ASD (C3I) and the Joint Staff.

Panel Member	Organization	Phone Number	E-Mail Address
Brian Wilczynski	US Navy (DON CIO)	703-607-5653	wilczynski.brian@hq.navy.mil
Bao Nguyen	US Air Force (AFCIC)	703-588-6310	NguyenB@pentagon.af.mil
Bruce Haberkamp	US Army (ODISC4)	703-614-0756	haberbw@hqda.army.mil
LCDR Bernadette Semple	US Navy (CNO N6)	703-601-1490	semple.bernadette@hq.navy.mil
LTC C. Chamberlain	J6	703-697-0857	chambelm@js.pentagon.mil
Scarlett Curry	ASD (C3I)	703-604-1574	CurryS@osd.pentagon.mil
Donna Cohen	IC CIO	703-267-2463	donna.cohen@eds.com
Nancy Lopez	DFAS	703-607-3956	nancy.lopez@dfas.mil
Andy Whitney	NIMA	703-755-5686	WhitneyA@nima.mil
	DISA		